



PCT/FR 2004 / 002734

REC'D 07 JAN 2005

WIPO

PCT

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 29 OCT. 2004

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE  
PRIORITÉ

PRÉSENTÉ OU TRANSMIS  
CONFORMÉMENT À LA RÈGLE  
17.1. a) OU b)

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint-Petersbourg  
75800 PARIS cedex 08  
Téléphone : 33 (0)1 53 04 53 04  
Télécopie : 33 (0)1 53 04 45 23  
www.inpi.fr

BEST AVAILABLE COPY



is, rue de Saint Pétersbourg - 75800 Paris Cedex 08

vous informer : INPI DIRECT

N° INPI 0 825 83 85 87

0,15 € TTC/mn

copie : 33 (0)1 53 04 52 65

Réservé à l'INPI

MISE DES PIÈCES  
TE

U

6 NOV 2003

75 INPI PARIS 34 SP

D'ENREGISTREMENT

0313034

TIONAL ATTRIBUÉ PAR L'INPI

TE DE DÉPÔT ATTRIBUÉE

- 6 NOV. 2003

R L'INPI

os références pour ce dossier

acullatif) 240690 D21317 MAA

# BREVET D'INVENTION CERTIFICAT D'UTILITÉ

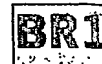
Code de la propriété intellectuelle - Livre VI



N° 11354\*03

## REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 @ W / 030103

**NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE  
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE**

Cabinet REGIMBEAU  
20, rue de Chazelles  
75847 PARIS CEDEX 17  
FRANCE

onfirmation d'un dépôt par télécopie

☐ N° attribué par l'INPI à la télécopie

**2 NATURE DE LA DEMANDE**

**Cochez l'une des 4 cases suivantes**

Demande de brevet

☒

Demande de certificat d'utilité

☐

Demande divisionnaire

☐

*Demande de brevet initiale*

N°

Date

*ou demande de certificat d'utilité initiale*

N°

Date

Transformation d'une demande de

brevet européen *Demande de brevet initiale*

N°

Date

**3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)**

PROCEDE DE CONTROLE AUTOMATIQUE DES FRAUDES DANS UN SYSTEME DE TRANSACTIONS  
ELECTRONIQUES

**4 DÉCLARATION DE PRIORITÉ**

**OU REQUÊTE DU BÉNÉFICE DE**

**LA DATE DE DÉPÔT D'UNE**

**DEMANDE ANTÉRIEURE FRANÇAISE**

Pays ou organisation

Date

N°

Pays ou organisation

Date

N°

Pays ou organisation

Date

N°

☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

**5 DEMANDEUR (Cochez l'une des 2 cases)**

☒ **Personne morale**

☐ **Personne physique**

Nom  
ou dénomination sociale

FRANCE TELECOM

Prénoms

Forme juridique

SOCIETE ANONYME

N° SIREN

380129866

Code APE-NAF

6, place d'Alleray, 75015 PARIS

Domicile

Rue

ou

siège

Code postal et ville

Pays

FRANCE

Française

Nationalité

N° de téléphone (facultatif)

N° de télécopie (facultatif)

Adresse électronique (facultatif)

☐ S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»

Remplir impérativement la 2<sup>ème</sup> page



# BREVET D'INVENTION CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE  
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES

DATE

6 NOV 2003

LIEU

75 INPI PARIS 34 SP

N° D'ENREGISTREMENT

0313034

NATIONAL ATTRIBUÉ PAR L'INPI

08 540 W / 030103

**6 MANDATAIRE (s'il y a lieu)**

Nom

240690 MAA

Prénom

Cabinet ou Société

Cabinet REGIMBEAU

N° de pouvoir permanent et/ou  
de lien contractuel

Adresse

Rue

20, rue de Chazelles

Code postal et ville

75847 PARIS CEDEX 17

Pays

N° de téléphone (facultatif)

01 44 29 35 00

N° de télécopie (facultatif)

01 44 29 35 99

Adresse électronique (facultatif)

info@regimbeau.fr

**7 INVENTEUR (S)**

Les inventeurs sont nécessairement des personnes physiques

Les demandeurs et les inventeurs  
sont les mêmes personnes☐ Oui☒ Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**8 RAPPORT DE RECHERCHE**

Uniquement pour une demande de brevet (y compris division et transformation)

Établissement immédiat  
ou établissement différé☒☐Paiement échelonné de la redevance  
(en deux versements)

Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt

☐ Oui☐ Non**9 RÉDUCTION DU TAUX  
DES REDEVANCES**

Uniquement pour les personnes physiques

☐ Requête pour la première fois pour cette invention (joindre un avis de non-imposition)☐ Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la  
décision d'admission à l'assistance gratuite ou indiquer sa référence): AG**10 SÉQUENCES DE NUCLEOTIDES  
ET/OU D'ACIDES AMINÉS**☐ Cochez la case si la description contient une liste de séquences

Le support électronique de données est joint

☐La déclaration de conformité de la liste de  
séquences sur support papier avec le  
support électronique de données est jointe☐Si vous avez utilisé l'imprimé «Suite»,  
indiquez le nombre de pages jointes**11 SIGNATURE DU DEMANDEUR  
OU DU MANDATAIRE**

(Nom et qualité du signataire)

94/102

VISA DE LA PRÉFECTURE  
OU DE L'INPI

L'invention concerne le domaine des services en ligne sur Internet ou tout autre réseau d'information.

5 Ces services mettent généralement en jeu des protocoles destinés à préserver la confidentialité des transactions électroniques réalisées. Notamment, ces services garantissent l'anonymat des utilisateurs par l'utilisation de clés de session. Lorsqu'un utilisateur se connecte à un service, une clé de session lui est attribuée. Cette clé est utilisée pour  
10 crypter les informations échangées entre l'utilisateur et le système fournisseur de services.

Certains systèmes de services en ligne disposent de moyens pour révéler la clé de session en cas d'utilisation frauduleuse du service. La révélation de la clé de session conduit à la révélation de l'identité de  
15 l'utilisateur malhonnête et par conséquent à la levée de l'anonymat de cet utilisateur.

Les moyens de levée d'anonymat d'utilisateurs mettent nécessairement en œuvre des moyens de détection aptes à commander la  
levée de l'anonymat si certaines conditions d'utilisation frauduleuse sont  
20 remplies. Ces moyens doivent donc être aptes à déterminer si il y a utilisation frauduleuse ou non.

Un but de l'invention est de fournir un système de levée d'anonymat dans le cadre d'un service en ligne qui ne nécessite pas de moyens pour déterminer une utilisation frauduleuse.

25 L'invention s'applique en cas d'utilisation frauduleuse consistant à obtenir un service un nombre de fois supérieur à ce qui est autorisé au cours d'une même session. C'est le cas par exemple, lorsqu'un utilisateur qui se connecte à un site de téléchargement de fichiers obtient le téléchargement de plusieurs fichiers alors qu'en réalité, il n'a payé que pour  
30 le téléchargement d'un seul fichier.

L'invention s'applique en particulier à la duplication illicite de biens électroniques.

L'invention propose un procédé de contrôle automatique des fraudes dans un système de transactions électroniques, caractérisé en ce qu'il comprend les étapes consistant à :

- lorsqu'un utilisateur initie une session dans le système de transaction électronique, générer un élément et enregistrer dans une base de données l'élément en association avec des informations identifiant l'utilisateur,
- à chaque fois qu'au cours de la session l'utilisateur commande la réalisation d'une opération, déterminer une équation à laquelle satisfait l'élément enregistré dans la base de données,
- lorsqu'un nombre suffisant donné d'opérations a été effectué, résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément,
- en se reportant à la base de données, déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur.

Dans le cadre de l'invention, une session est définie comme une période de temps au cours de laquelle un utilisateur est en relation avec un service en ligne donné et est autorisé par le fournisseur du service à réaliser un certain nombre d'opérations données.

Le procédé de l'invention conduit à révéler l'identité d'un utilisateur lorsque celui-ci a réalisé un nombre  $n$  donné d'opérations au cours d'une même session alors qu'il n'y était pas autorisé par le fournisseur de services.

Le procédé de l'invention s'applique automatiquement et de la même manière à tous les utilisateurs d'un service donné. Il n'y a donc aucune distinction d'application entre utilisateurs frauduleux et utilisateurs normaux. Le procédé de l'invention ne met donc pas en œuvre de moyens spécifiques en cas d'utilisation frauduleuse.

Par ailleurs, avec le procédé de l'invention, l'identité de l'utilisateur n'est divulguée que lorsque celui-ci réalise un nombre donné  $n$  d'opérations supérieur au nombre d'opérations autorisé, au cours d'une même session. Par conséquent, avant que l'utilisateur ne réalise la  $n$ -ième opération, le procédé ne donne aucune indication quant à l'identité de l'utilisateur

puisqu'il fournit un certain nombre d'équations et qu'il existe une infinité de solutions satisfaisant ces équations. Il en résulte que le procédé de l'invention permet de préserver totalement l'anonymat des utilisateurs tant que ceux-ci respectent les limites définies par le fournisseur de services.

5 De préférence, les équations du système d'équations sont indépendantes. Ainsi, l'utilisateur sera systématiquement identifié lorsqu'il aura réalisé un nombre  $n$  connu d'opérations, le nombre  $n$  correspondant au nombre d'opérations nécessaires pour obtenir un système de  $n$  équations conduisant à une solution unique.

10 Les équations peuvent être des équations linéaires.

L'élément est par exemple constitué d'une série de coefficients numériques.

Ces coefficients numériques peuvent avantageusement définir un objet géométrique tel qu'un point, une droite, un hyperplan, etc. dans un  
15 espace à  $n$  dimensions.

Ils peuvent également définir un objet mathématique tel qu'une fonction, une suite, etc.

L'invention concerne également un système de contrôle automatique des fraudes dans un système de transactions électroniques,  
20 caractérisé en ce qu'il comprend des premiers moyens de calcul pour générer un élément lorsqu'un utilisateur initie une session dans le système de transactions électroniques, une base de données dans laquelle est enregistré l'élément en association avec des informations identifiant l'utilisateur, les premiers moyens de calcul étant aptes à déterminer une  
25 équation à laquelle satisfait l'élément enregistré dans la base de données à chaque fois qu'au cours de la session l'utilisateur commande la réalisation d'une opération, et des seconds moyens de calcul aptes à résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément lorsqu'un nombre suffisant donné d'opérations a été  
30 effectué, de sorte qu'en se reportant à la base de données, il soit possible de déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur.

D'autres caractéristiques et avantages ressortiront encore de la description qui suit, laquelle est purement illustrative et non limitative et doit être lue en regard des figures annexées parmi lesquelles :

- la figure 1 représente un exemple de système conforme à une  
5 mise en œuvre de l'invention,

- la figure 2 est une représentation graphique de la détermination d'un élément associé à un utilisateur, l'élément étant une droite définie dans un espace à 2 dimensions,

- la figure 3 est une représentation graphique de la détermination  
10 d'un élément associé à un utilisateur, l'élément étant un plan défini dans un espace de dimension  $n=3$ ,

- la figure 4 est une représentation graphique de la détermination d'un élément associé à un utilisateur, l'élément étant un point défini dans un espace à 2 dimensions,

15 - la figure 5 est une représentation graphique de la détermination d'un élément associé à un utilisateur, l'élément étant un point défini dans un espace de dimension  $n=3$ .

Sur la figure 1, le système de contrôle des fraudes 100 est associé à un serveur 200 de services en ligne (par exemple service de  
20 téléchargement de fichiers ou de programmes, service d'achats en ligne, service de consultation de documents, service de communication, etc.) détenu par un fournisseur de services. Le système de contrôle des fraudes comprend un module de pilotage 102 relié au serveur 200, une base de données 104 reliée au module de pilotage 102, un générateur pseudo-  
25 aléatoire 106, un premier module de calcul 108 et un deuxième module de calcul 110. Le générateur pseudo-aléatoire 106, le premier module de calcul 108 et un deuxième module de calcul 110 sont commandés par le module de pilotage 102.

Selon une première mise en œuvre du système de l'invention,  
30 lorsqu'un utilisateur 300 se connecte au serveur 200 du fournisseur de services via un réseau de communication 400 et ouvre une session, une clé de session temporaire est automatiquement attribuée à l'utilisateur par le serveur. La clé de session est enregistrée dans la base de données 104.

Elle est normalement conservée dans la base de données 104 durant toute la durée de la session, puis supprimée lors de la fermeture de la session. Elle permet un échange sécurisé entre l'utilisateur 300 et le serveur 200. Les clés et autres informations contenues dans la base de données 104 sont confidentielles.

Par ailleurs, lorsque l'utilisateur 300 ouvre une session, le premier module de calcul 108 génère une équation de droite (dimension 1) dans un espace de dimension 2, l'équation étant du type  $Y = aX + b$ . L'équation de droite est enregistrée dans la base de données 104 en association avec la clé de session attribuées à l'utilisateur. Ainsi, l'utilisateur et la session sont associés de manière univoque à la droite D définie par le couple de coefficients (a, b).

Lorsque l'utilisateur commande la réalisation d'une opération particulière (par exemple téléchargement d'un fichier ou d'un programme) dans le cadre de la session qu'il a ouverte, le premier module de calcul 108 détermine les coordonnées d'un point  $P_1 (X_1, Y_1)$  appartenant à la droite D. A cet effet, le module de pilotage commande le générateur pseudo-aléatoire 106 pour que celui-ci génère une première coordonnée  $X_1$ . A partir de cette coordonnée  $X_1$ , le premier module de calcul 108 détermine une deuxième coordonnée  $Y_1$  à partir de l'équation de la droite D, telle que :

$$Y_1 = aX_1 + b$$

Ce premier point  $P_1 (X_1, Y_1)$  seul ne permet pas de déterminer l'équation de la droite D. A ce stade, il n'est pas possible de remonter à l'identité de l'utilisateur 300.

Si l'utilisateur 300 réussit de manière illicite à commander la réalisation d'une autre opération au cours de la même session, le premier module de calcul 108 détermine les coordonnées d'un deuxième point  $P_2 (X_2, Y_2)$  appartenant à la droite D. A cet effet, le module de pilotage 102 commande le générateur pseudo-aléatoire 106 pour que celui-ci génère une première coordonnée  $X_2$  différente de  $X_1$ . A partir de cette coordonnée  $X_2$ , le premier module de calcul 108 détermine une deuxième coordonnée  $Y_2$  à partir de l'équation de la droite D, telle que :

$$Y_2 = aX_2 + b$$

Ainsi qu'illustré sur la figure 2, à partir des deux points  $P_1 (X_1, Y_1)$  et  $P_2 (X_2, Y_2)$  ainsi déterminés, le deuxième module de calcul 110 en déduit l'équation de la droite D. A cet effet, le deuxième module résout le système

5 d'équations suivant :

$$\begin{cases} Y_1 = aX_1 + b \\ Y_2 = aX_2 + b \end{cases}$$

Connaissant l'équation de la droite D (c'est à dire les coefficients a et b) fournie par le deuxième module de calcul 110, le module de pilotage 102 en déduit, en se reportant à la base de données 104, la clé de session associée. Cette clé permet d'identifier l'utilisateur frauduleux qui a obtenu la réalisation de deux opérations alors même qu'il était autorisé qu'à n'en réaliser qu'une.

10 Lorsque la confidentialité de l'identité de l'utilisateur 300 a été levée, plusieurs étapes peuvent ensuite être mises en œuvre. Le fournisseur de services peut par exemple interdire à l'utilisateur 300 l'accès au serveur 200.

Dans la mise en œuvre de l'invention décrite précédemment, l'espace dans lequel sont créées des droites est un espace de dimension 2. Cette mise en œuvre peut être généralisée à une application dans un espace de dimension n.

20 Le premier module de calcul 108 génère une équation d'un hyperplan H (dimension n-1) dans un espace E de dimension n, l'équation étant du type  $X_n = a_{n-1}X_{n-1} + \dots + a_2X_2 + a_1X_1 + a_0$ , dans laquelle au moins (n-2) coefficients parmi  $a_{n-1}, \dots, a_2, a_1, a_0$  sont nuls. La clé de session ainsi que l'équation d'hyperplan H associé sont enregistrés dans la base de données 104. Ainsi, l'utilisateur et la session sont associés à l'hyperplan H défini par le n-uplet de coefficients  $(a_{n-1}, \dots, a_2, a_1, a_0)$ .

A chaque fois que l'utilisateur commande la réalisation d'une i-ème opération au cours de la même session, le premier module de calcul 108 détermine un point  $P_i$  de coordonnées  $(X_i^1, X_i^2, \dots, X_i^n)$  appartenant à

l'hyperplan H. A cet effet, le module de pilotage 102 commande le générateur pseudo-aléatoire 106 pour que celui-ci génère un (n-1)-uplet de coordonnées  $(X_i^1, X_i^2, \dots, X_i^{n-1})$ . A partir de ce (n-1)-uplet, le premier module de calcul 108 détermine une n-ième coordonnée  $X_i^n$  en se référant à

5 l'équation de l'hyperplan H, telle que :

$$X_i^n = a_{n-1}X_i^{n-1} + \dots + a_2X_i^2 + a_1X_i^1 + a_0$$

Lorsque l'utilisateur 300 a commandé pour la n-ième fois la réalisation d'une opération au cours de la même session, le deuxième module de calcul 110 déduit l'équation de l'hyperplan H à partir des n points

10  $P_1, P_2, \dots, P_n$  calculés par le premier module de calcul 108. A cet effet, il résout le système d'équations suivant :

$$\begin{cases} X_1^n = a_{n-1}X_1^{n-1} + \dots + a_2X_1^2 + a_1X_1^1 + a_0 \\ X_2^n = a_{n-1}X_2^{n-1} + \dots + a_2X_2^2 + a_1X_2^1 + a_0 \\ \dots \\ X_n^n = a_{n-1}X_n^{n-1} + \dots + a_2X_n^2 + a_1X_n^1 + a_0 \end{cases}$$

Connaissant l'équation de l'hyperplan H (c'est à dire les coefficients  $a_{n-1}, \dots, a_2, a_1, a_0$ ), il est possible, en se reportant à la base de données 104

15 d'en déduire la clé de session associée à cet hyperplan H et par conséquent de remonter à l'identité de l'utilisateur frauduleux. Cette clé permet d'identifier l'utilisateur frauduleux qui a obtenu la réalisation de n opérations alors même qu'il était autorisé qu'à n'en réaliser que n-1.

La figure 3 représente la détermination d'un plan H (dimension 2)

20 dans un espace de dimension n=3 à partir de 3 points  $P_1, P_2$  et  $P_3$  calculés par le premier module de calcul 108.

Selon un deuxième mode de mise en œuvre du système de contrôle des fraudes, lorsqu'un utilisateur 300 se connecte au serveur 200 du fournisseur de services via un réseau de communication 400 et ouvre

25 une session, une clé de session temporaire est automatiquement attribuée à l'utilisateur 300 par le serveur 200.

Le premier module de calcul 108 génère un point P (dimension 0) dans un espace de dimension 2. Le point étant défini par des coordonnées du type (X, Y). La clé de session ainsi que les coordonnées du point P associées sont enregistrées dans la base de données.

- 5 Lorsque l'utilisateur commande la réalisation de l'opération, le premier module de calcul détermine une équation  $Y=a_1X+b_1$  d'une droite  $D_1$  passant par le point P (X, Y). A cet effet, le module de pilotage commande le générateur pseudo-aléatoire pour que celui-ci génère un premier coefficient  $a_1$  correspondant à la pente de la droite  $D_1$ . A partir de ce
- 10 coefficient  $a_1$ , le premier module de calcul détermine un deuxième coefficient  $b_1$  correspondant à l'ordonnée à l'origine de la droite  $D_1$  à partir des coordonnées (X, Y) tel que  $Y=a_1X+b_1$ . On a :

$$b_1 = Y - a_1 \cdot X$$

- Cette première équation de droite  $Y=a_1X+b_1$  ne permet pas de
- 15 déterminer les coordonnées du point P (X, Y) et de remonter à l'identité de l'utilisateur.

- Ainsi qu'illustré sur la figure 4, si l'utilisateur commande de manière illicite la réalisation de la même opération, le premier module détermine une équation  $Y=a_2X+b_2$  d'une deuxième droite  $D_2$  passant pas le point (X, Y). A
- 20 cet effet, le module de pilotage commande le générateur pseudo-aléatoire pour que celui-ci génère un premier coefficient  $a_2$  différent de  $a_1$ . A partir de ce coefficient  $a_2$ , le premier module de calcul détermine un deuxième coefficient  $b_2$  à partir des coordonnées du point (X, Y) tel que :

$$b_2 = Y - a_2 \cdot X$$

- 25 Dans cette mise en œuvre de l'invention, l'espace dans lequel sont créés les points est un espace de dimension 2. Cette mise en œuvre peut être généralisée à une application dans un espace de dimension n.

- Lorsque l'utilisateur commande la réalisation d'une opération particulière (par exemple téléchargement d'un fichier ou d'un programme)
- 30 dans le cadre de la session qu'il a ouverte, le premier module de calcul 108 génère un point P (dimension 0) dans un espace de dimension n. La clé de session ainsi que le point P associé à cette clé sont enregistrés dans la

base de données 104. Ainsi, l'utilisateur et la session sont associés à un point P défini par le n-uplet de coordonnées  $(X_1, X_2, \dots, X_n)$ .

A chaque fois que l'utilisateur commande la réalisation d'une i-ème opération au cours de la même session, le premier module de calcul 108 détermine un hyperplan  $H_i$  contenant le point P  $(X_1, X_2, \dots, X_n)$ , l'hyperplan  $H_i$  étant défini par une équation du type  $X^n = a_{n-1}^i X^{n-1} + \dots + a_2^i X^2 + a_1^i X^1 + a_0^i$ , dans laquelle au moins (n-2) coefficients parmi les coefficients  $a_{n-1}^i, \dots, a_2^i, a_1^i, a_0^i$  sont nuls. A cet effet, le module de pilotage commande le générateur pseudo-aléatoire 106 pour que celui-ci génère un (n-1)-uplet de coefficients  $(a_1^i, a_2^i, \dots, a_{n-1}^i)$ . A partir de ce (n-1)-uplet, le premier module de calcul 108 détermine un n-ième coefficient  $a_0^i$  à partir des coordonnées du point P  $(X_0, X_1, X_2, \dots, X_n)$ , tel que :

$$X_n = a_{n-1}^i X_{n-1} + \dots + a_2^i X_2 + a_1^i X_1 + a_0^i$$

L'anonymat de l'utilisateur 300 est maintenu tant que celui-ci réalise au plus (n-1) opérations car le système génère (n-1) équations à n inconnues, les n inconnues étant les coordonnées  $(X_1, X_2, \dots, X_n)$  du point P.

Lorsque l'utilisateur 300 réalise n opérations au cours de la même session, le deuxième module de calcul 110 déduit les coordonnées du point P  $(X_1, X_2, \dots, X_n)$  comme étant l'intersection des n hyperplans  $H_1, H_2, \dots, H_n$  calculés par le premier module de calcul 108. A cet effet, le deuxième module de calcul 110 résout un système de n équations à n inconnues :

$$\begin{cases} X_n = a_{n-1}^1 X_{n-1} + \dots + a_2^1 X_2 + a_1^1 X_1 + a_0^1 \\ X_n = a_{n-1}^2 X_{n-1} + \dots + a_2^2 X_2 + a_1^2 X_1 + a_0^2 \\ \dots \\ X_n = a_{n-1}^n X_{n-1} + \dots + a_2^n X_2 + a_1^n X_1 + a_0^n \end{cases}$$

Connaissant les coordonnées du point P  $(X_1, X_2, \dots, X_n)$ , il est possible, en se reportant à la base de données 104 d'en déduire la clé de

session associée à ce point P et par conséquent de remonter à l'identité de l'utilisateur frauduleux.

La figure 5 représente la détermination du point P dans un espace de dimension  $n=3$  à partir de 3 plans  $H_1$ ,  $H_2$  et  $H_3$  (dimension 2) calculés par le premier module de calcul 108.

## REVENDICATIONS

1. Procédé de contrôle automatique des fraudes dans un système de transactions électroniques, caractérisé en ce qu'il comprend les étapes consistant à :
  - lorsqu'un utilisateur initie une session dans le système de transaction électronique, générer un élément et enregistrer dans une base de données l'élément en association avec des informations identifiant l'utilisateur,
  - à chaque fois qu'au cours de la session l'utilisateur commande la réalisation d'une opération, déterminer une équation à laquelle satisfait l'élément enregistré dans la base de données,
  - lorsqu'un nombre suffisant donné d'opérations a été effectué, résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément,
  - en se reportant à la base de données, déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur.
2. Procédé selon la revendication 1, caractérisé en ce que les équations du système d'équations sont indépendantes.
3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que les équations sont des équations linéaires.
4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que l'élément est constitué d'une série de coefficients numériques.
5. Procédé selon la revendication 4, caractérisé en ce que la série de coefficients définit une équation d'hyperplan (H) de dimension (n-1) dans un espace (E) de dimension n et en ce que, à chaque fois que l'utilisateur commande la réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer les coordonnées  $(X_i^1, X_i^2, \dots, X_i^n)$  d'un point (Pi) appartenant à l'hyperplan (H).
6. Procédé selon la revendication 5, caractérisé en ce que la série de coefficients définit une équation de droite (D) dans un espace (E) à 2 dimensions et en ce que, à chaque fois que l'utilisateur commande la

réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer les coordonnées  $(X_i, Y_i)$  appartenant à cette droite  $(D)$ .

7. Procédé selon la revendication 4, caractérisé en ce que la série de coefficients définit les coordonnées  $(X_1, X_2, \dots, X_n)$  d'un point  $(P)$  dans un espace  $(E)$  de dimension  $n$ , et en ce que, à chaque fois que l'utilisateur commande la réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer l'équation d'un hyperplan  $(H_i)$  contenant le point  $P$ .

8. Procédé selon la revendication 7, caractérisé en ce que la série de coefficients définit les coordonnées  $(X_1, X_2)$  d'un point  $(P)$  dans un espace  $(E)$  à 2 dimensions et en ce que, à chaque fois que l'utilisateur commande la réalisation d'une opération, l'étape de détermination d'une équation consiste à déterminer l'équation d'une droite  $(D_i)$  passant par le point  $P$ .

9. Système de contrôle automatique des fraudes dans un système de transactions électroniques, caractérisé en ce qu'il comprend des premiers moyens de calcul (108) pour générer un élément lorsqu'un utilisateur (300) initie une session dans le système de transaction électronique (200), une base de données (104) dans laquelle est enregistré l'élément en association avec des informations identifiant l'utilisateur, les premiers moyens de calcul (108) étant aptes à déterminer une équation à laquelle satisfait l'élément enregistré dans la base de données (104) à chaque fois qu'au cours de la session l'utilisateur (300) commande la réalisation d'une opération, et des seconds moyens de calcul (110) aptes à résoudre le système d'équations constitué des équations ainsi déterminées pour en déduire l'élément lorsqu'un nombre suffisant donné  $(n)$  d'opérations a été effectué, de sorte qu'en se reportant à la base de données (104), il soit possible de déduire à partir de l'élément obtenu, les informations correspondantes identifiant l'utilisateur (300).

1/3

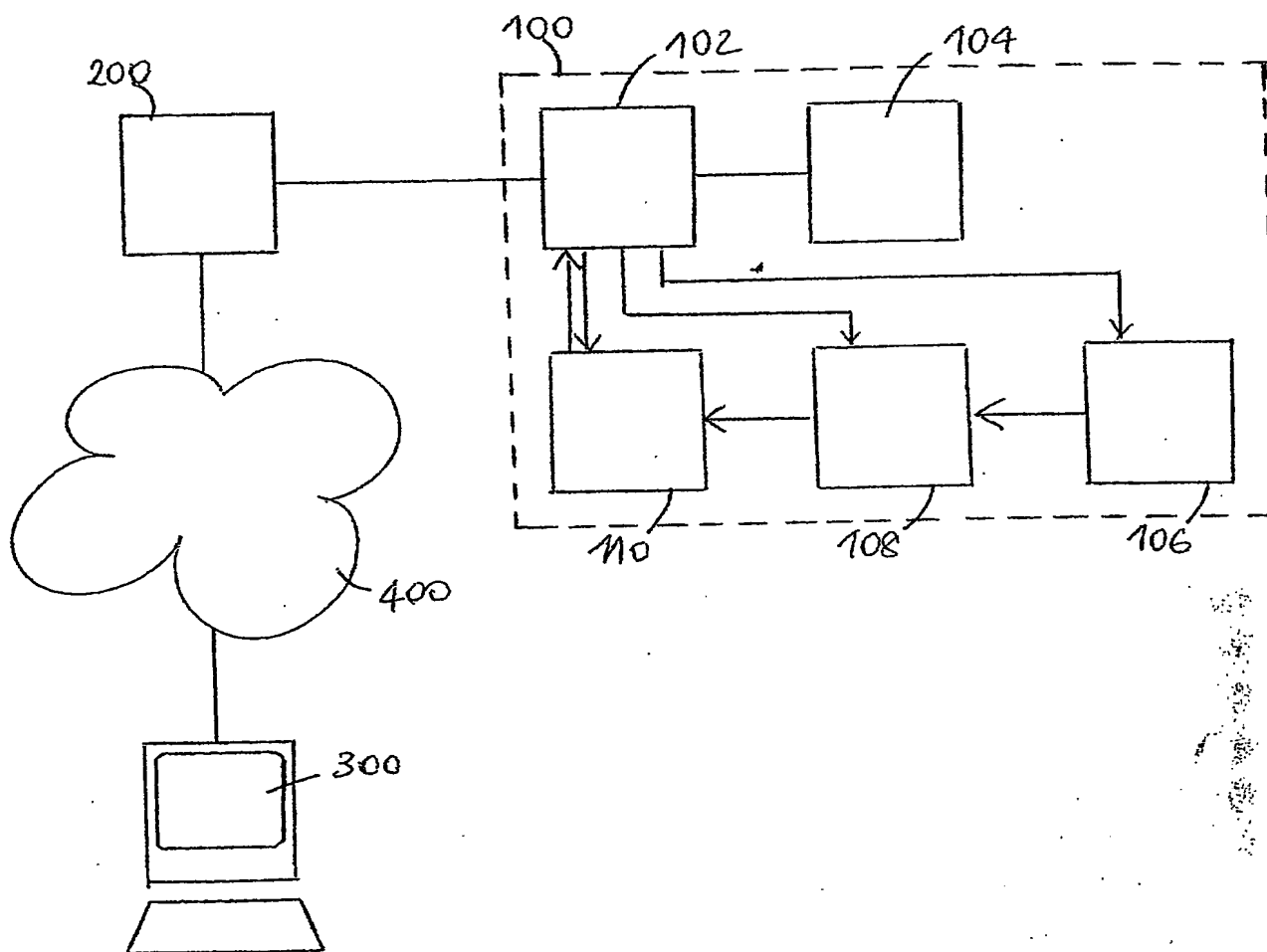


Figure 1



2 | 3

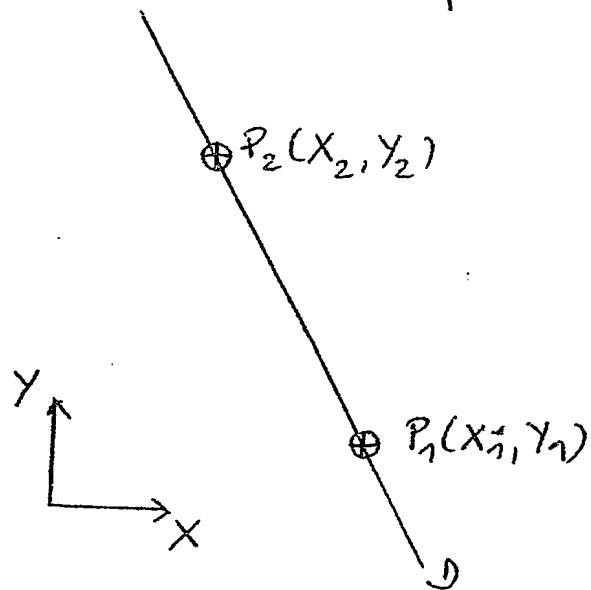


Figure 2

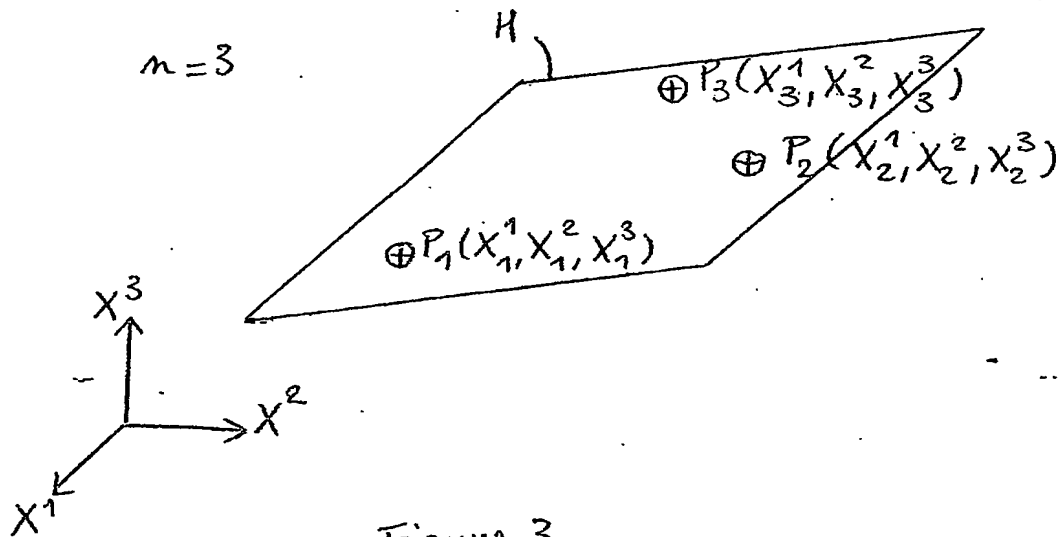


Figure 3

2/3

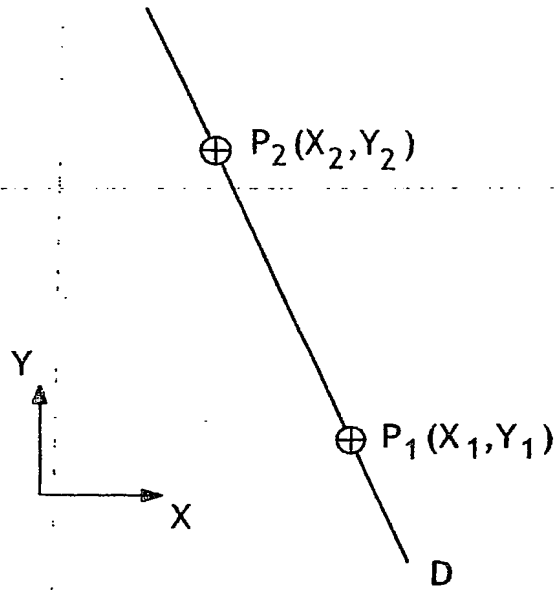


FIG.2

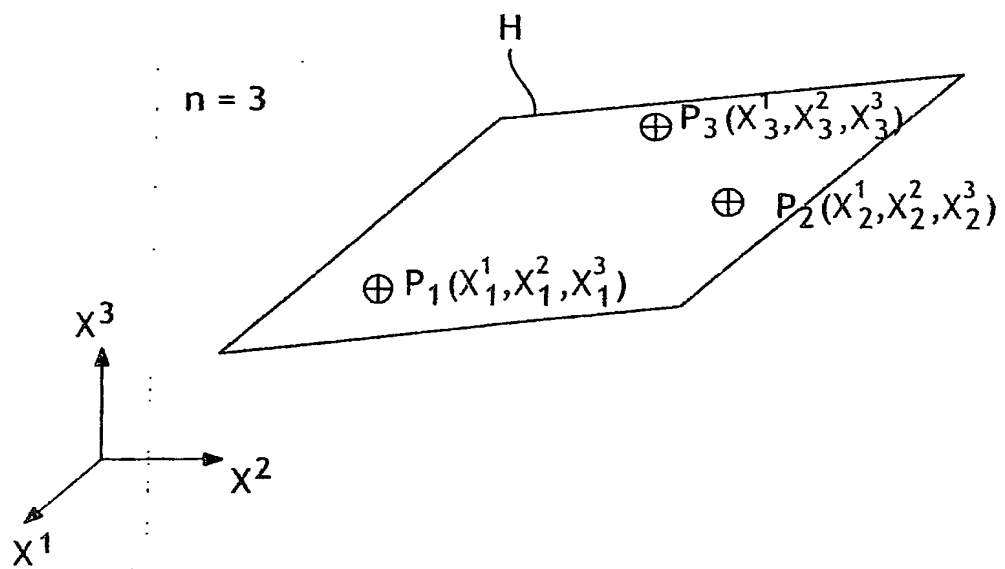


FIG.3

3/3

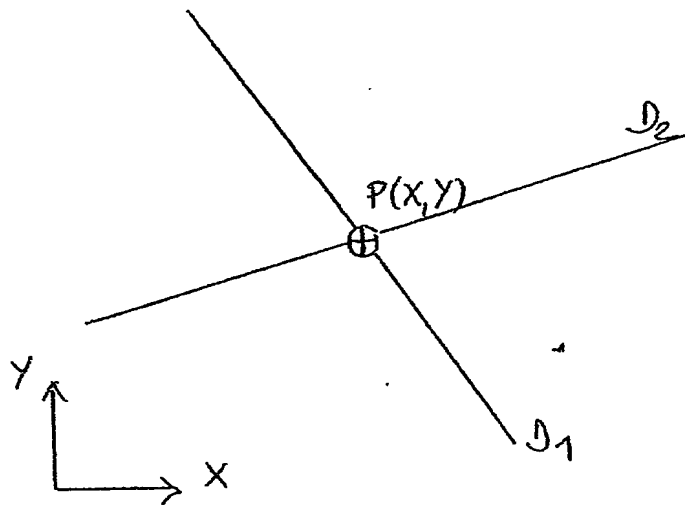


Figure 4

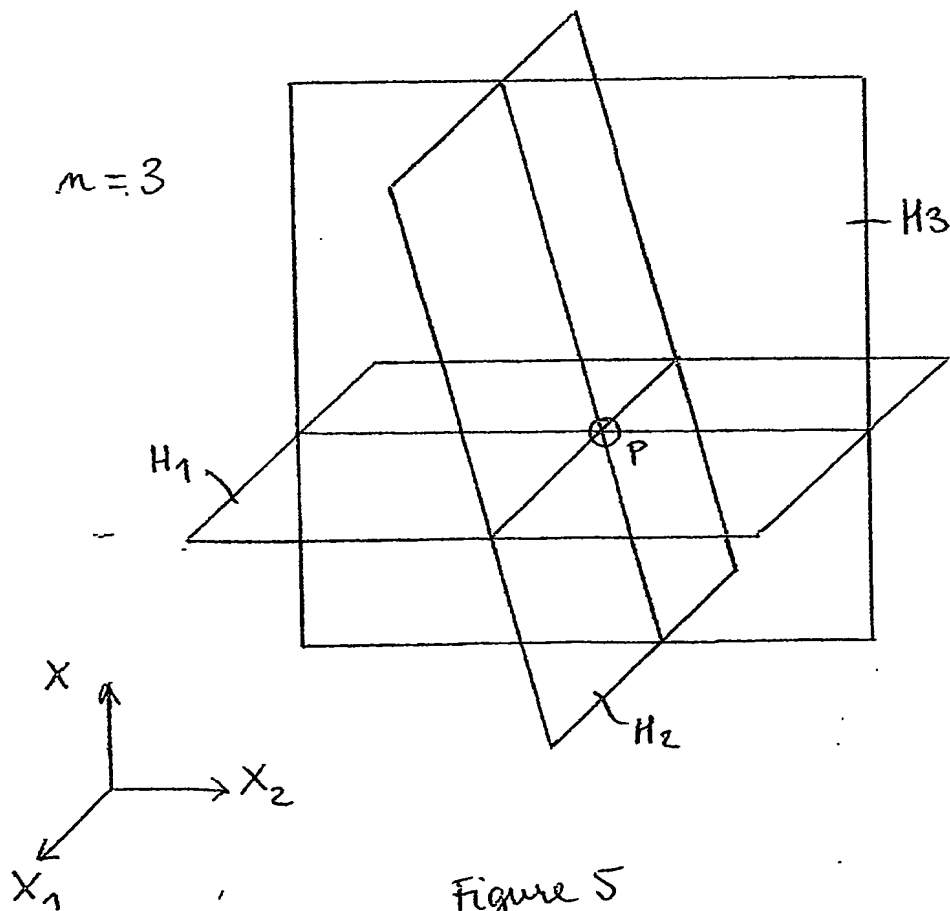


Figure 5

3 / 3

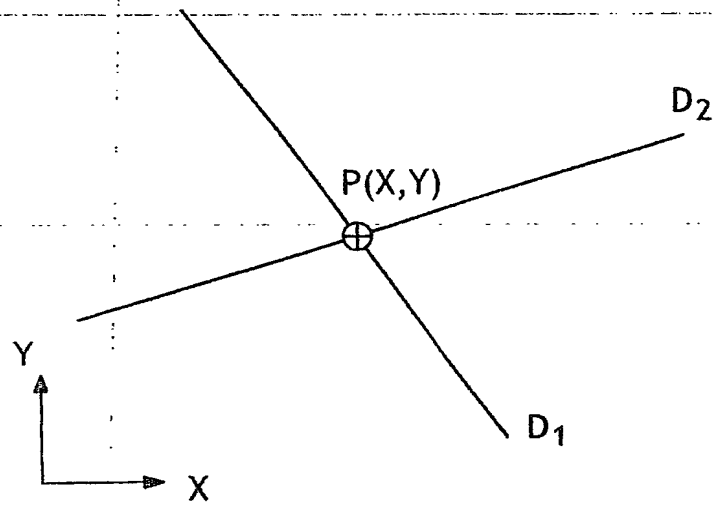


FIG.4

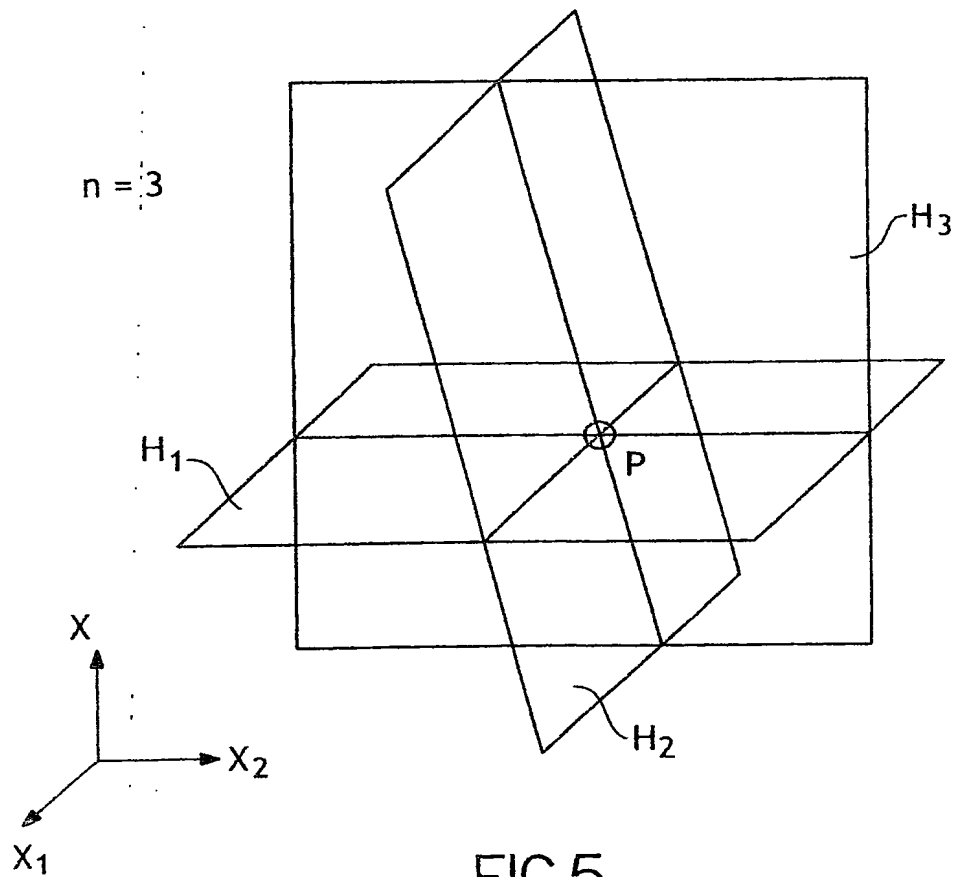


FIG.5

REMENT DES BREVETS

, rue de Saint Pétersbourg

Paris Cedex 08

phone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

**DÉSIGNATION D'INVENTEUR(S)** Page N° 1 / 1

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)



Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 270601

références pour ce dossier (facultatif)	
D'ENREGISTREMENT NATIONAL	0313034 240690 D21317 MAA
TITRE DE L'INVENTION (200 caractères ou espaces maximum)	

PROCÉDE DE CONTROLE AUTOMATIQUE DES FRAUDES DANS UN SYSTEME DE  
TRANSACTIONS ELECTRONIQUES

**(S) DEMANDEUR(S) :**

FRANCE TELECOM : 6, place d'Alleray, 75015 PARIS - FRANCE

**DESIGNE(NT) EN TANT QU'INVENTEUR(S) :**

Nom		
Prénoms		CLERC Fabrice
Adresse	Rue	2, place Alexandre Dumas
	Code postal et ville	14450 BLAINVILLE SUR ORNE - FRANCE
Société d'appartenance (facultatif)		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

**DATE ET SIGNATURE(S)**  
**DU (DES) DEMANDEUR(S)**  
**OU DU MANDATAIRE**  
(Nom et qualité du signataire)

06/11/03

guez

*W. B. L. Ch*

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record.**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: \_\_\_\_\_**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**